BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

December 22, 1997

Mr. Griffith L. Garwood
Director, Division of Consumer and Community Affairs

We are pleased to present our *Report on the Audit of the Division of Consumer and Community Affairs' Distributed Processing Environment* (A9704). We performed this audit to determine if the Division of Consumer and Community Affairs (C&CA) has established effective processes for planning, organizing, directing, and controlling the activities related to distributed processing; adequately managed the efficiency of its local area networks and developed an effective problem management system; properly secured its distributed systems and data; and developed appropriate backup and disaster recovery procedures.

Overall, we found that C&CA is taking steps to implement effective processes for planning, organizing, directing, and controlling its distributed processing environment. C&CA has established a central information systems team dedicated to office automation and application development, and we found that managers and staff were generally satisfied with the support and assistance provided by this team. C&CA uses innovative approaches to train and support its staff and division participation in System, Board, and interagency information technology efforts is noteworthy.

Notwithstanding this progress, we are concerned that C&CA has deferred its responsibility for network and security administration to the Division of Information Resources Management (IRM) without clearly defining performance expectations or ensuring that IRM is effectively addressing C&CA requirements. We believe that C&CA would benefit from having a broader view of its distributed processing program and that an automation strategic plan would help C&CA ensure that it has the technical infrastructure required to effectively and efficiently meet its current and emerging business needs. To help free up resources to focus on more strategic issues, we believe that C&CA should streamline certain aspects of its office automation support. Finally, we found that the security and general controls over C&CA's distributed processing environment need to be strengthened. Although this report focuses on C&CA, we have had similar findings in reviewing other divisions' distributed processing environments.

We provided a draft of this report for your review and comment. This report incorporates your response which indicates general agreement with our findings and recommendations. Your response also reflects C&CA's position that some of the points raised in our report are the result of systemic issues that could be more efficiently addressed on a Boardwide basis, and C&CA's expectation that IRM should be proactive in providing at least a basic level of service. While your point has merit, we continue to emphasize that, as the information owner, C&CA is ultimately responsible for managing its information resources and ensuring compliance with policies and safeguards.

A copy of this report is being sent to members of the Board's Committee on Consumer and Community Affairs, the Vice Chair as Administrative Governor, and selected Board staff. The report is available to the public on our internet web page at *http://www.ignet.gov/ignet* and a summary will appear in our next semiannual report to Congress. We plan to follow up on implementation of our recommendations and will report any exceptions as part of our future audit activities.

Sincerely,

Barry R. Snyder
Assistant Inspector General for Audits

Enclosure

Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF CONSUMER AND COMMUNITY AFFAIRS' DISTRIBUTED PROCESSING ENVIRONMENT

OFFICE OF INSPECTOR GENERAL

(A9704) December 1997

TABLE OF CONTENTS

Page

BACKGROUND

Over the past several years, the Board of Governors of the Federal Reserve System (the Board) has shifted its resources to provide analytical tools to users at their desktops, while reserving larger scale processing and storage functions for the mainframe and larger distributed servers. Shifting to the desktop computing environment offers the user a powerful set of tools for data handling; at the same time, however, operational management functions of distributed systems such as security, backup and recovery, problem resolution, and performance management may not be as fully developed as their mainframe counterparts. While these operational functions may pose potential control weaknesses, the weaknesses can be overcome by effectively managing and securing distributed office automation systems and their associated local area networks (LANs).[1]

To provide policy direction regarding the protection of its information assets, the Federal Reserve System (the System) recently issued the *Information Security Manual* (ISM), which defines the security policies and safeguards for information security and is applicable to all automated platforms and manual processes used throughout the System.[2] Two additional manuals—the *Distributed Processing Security Support Manual* and the *Mainframe and FEDNET Security Support Manual*—provide more specific policies and procedures directly related to the indicated data processing environment. Board divisions and offices were expected to comply with the policies and safeguards in these manuals as of January 1, 1997.

The Division of Consumer and Community Affairs' Distributed Processing Environment

The Board is responsible for implementing a number of federal laws intended to protect consumers in credit and other financial transactions and to ensure that commercial banks comply with these laws and regulations. The Division of Consumer and Community Affairs (C&CA) supports the Board in carrying out these responsibilities. Specifically, C&CA prepares and interprets regulatory material to strike a balance between protection of consumers and costs to the industry; analyzes and develops proposals to improve federal consumer credit protection laws; supports and oversees the supervisory efforts of the Reserve Banks to ensure that compliance with the laws is fully and fairly enforced; processes consumer complaints and reviews System complaint-processing activity to ensure prompt and equitable treatment of the public; reviews bank and bank holding company

[1] A local area network is a group of computers and other devices that are connected to exchange information and are typically dispersed throughout a small area, such as a building or office. A LAN can be connected to a larger network.

[2] "System" is used throughout the report to refer to the Board and the Federal Reserve Banks and their respective offices.

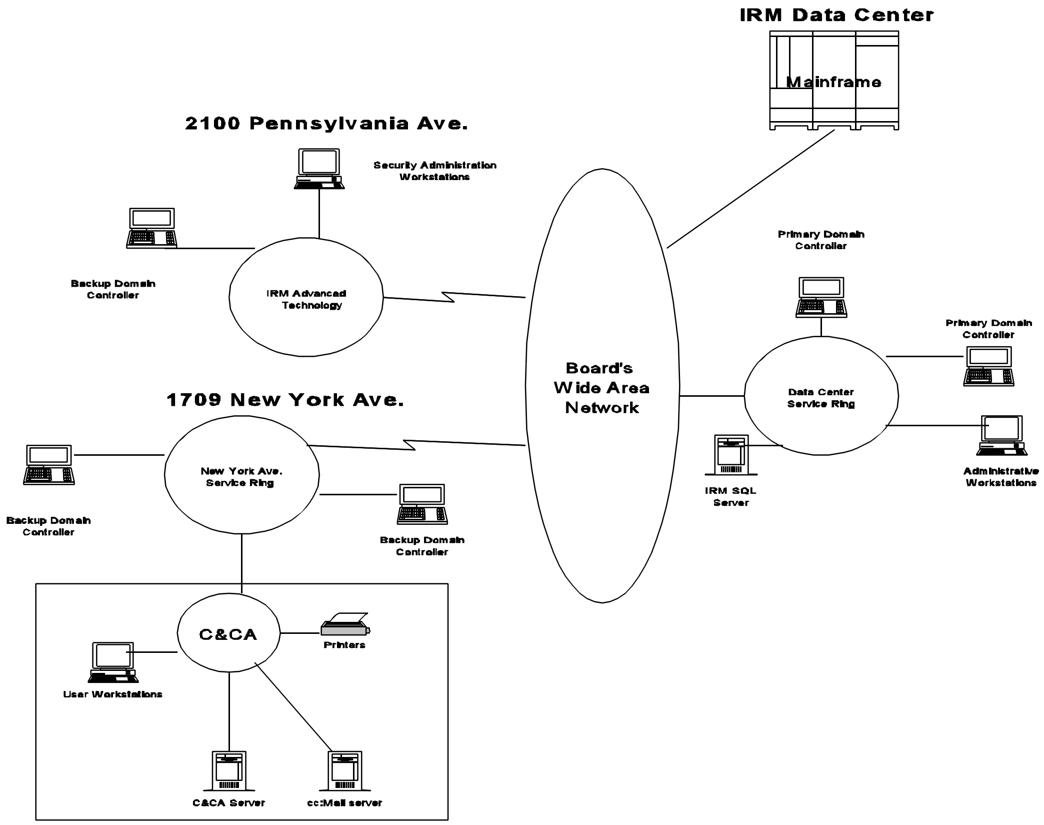
applications with respect to adverse Community Reinvestment Act of 1977 (CRA) and compliance issues; and assists and monitors the community affairs activity of the Federal Reserve System.[3]

To support its mission, C&CA has a distributed processing system that includes a server, eighty-five workstations, and eleven printers. Its system is a subset of the Board's wide area network, which provides connectivity to the mainframe, other LANs, the Board and System Intranets, and the Internet (see figure 1). The C&CA server supports eleven different distributed software products developed specifically for the division. C&CA's workstations are used for office automation tasks, such as word processing and spreadsheets, electronic mail, and data downloading. Through the Board's wide area network, users also have access to services—such as electronic mail, the Internet, on-line research services, and dial-in access—and to the Board's Division of Information Resources Management's (IRM's) Structure Query Language (SQL) servers, which are located in the data center. These SQL servers provide Home Mortgage Disclosure Act of 1975 (HMDA) data and other data that is used to assess (a) lending patterns to ensure fair and equal access to credit and (b) inquiries and complaints from consumers to monitor banking and CRA trends and consumer issues.[4] Effective July 1, 1997, C&CA's desktop PC operating system standard became Microsoft's Windows 95/ Windows New Technology (Windows NT), and Windows 95 for portable PCS. Effective January 1, 1998, the software application standard will be Microsoft Office. C&CA is converting to these software standards within the specified time frames.

[3] The Community Reinvestment Act of 1977 encourages financial institutions to help meet the credit needs of their communities, particularly low- and moderate-income neighborhoods.

[4] The Home Mortgage Disclosure Act of 1975 (HMDA) requires mortgage lenders to publicly disclose the geographic distribution of their mortgage and home improvement loans and their loan approval rates by sex, race, and other applicant characteristics.

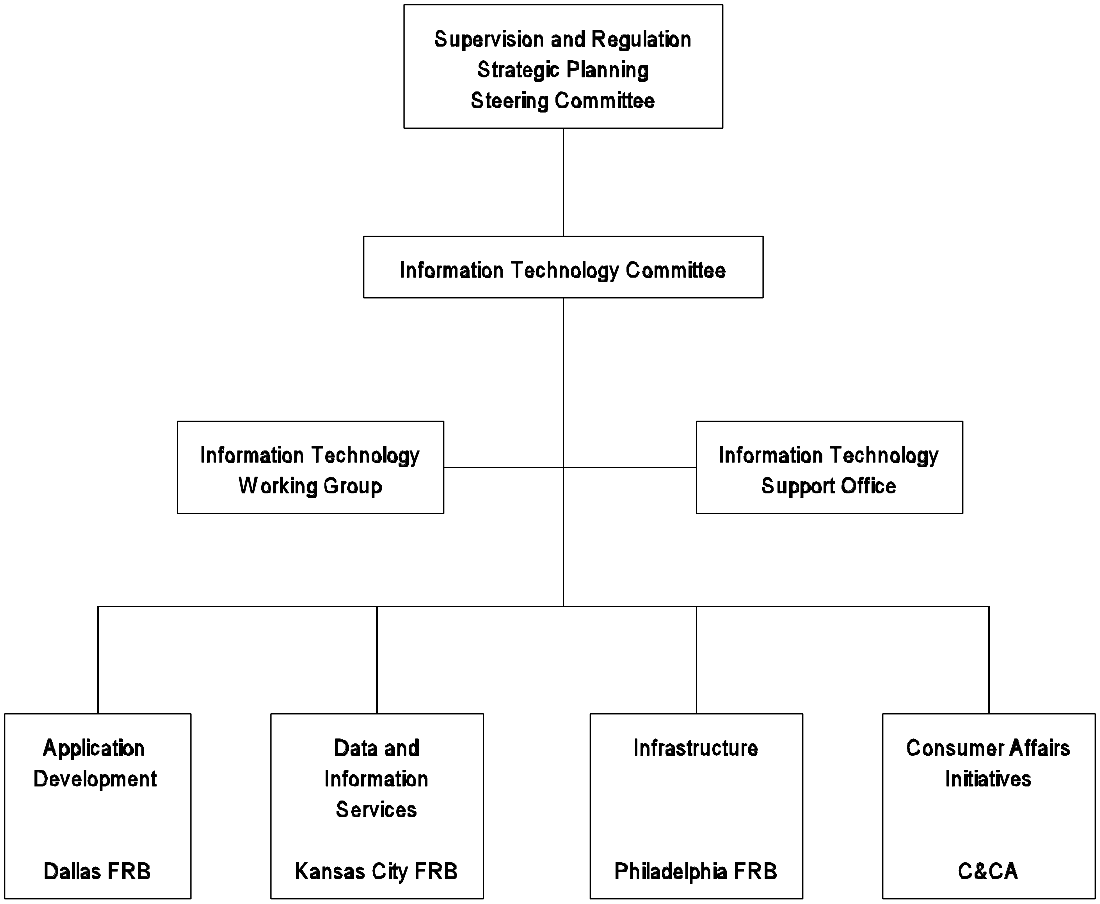
Figure 1
High-Level Diagram of C&CA's Distributed Processing Environment



C&CA Information Technology Management and Support Structure

C&CA is committed to using information technology to manage the vast amounts of information used to carry out its supervisory and regulatory mission and is an active participant in the information technology framework, through its roles and responsibilities on various committees and working groups. The Director of C&CA is an advisory member to the Supervision and Regulation Strategic Planning Steering Committee, and C&CA heads the Consumer Affairs Initiatives Office as part of its membership on the Information Technology Committee (ITC), a key subgroup of the Steering Committee (see figure 2). The ITC coordinates the acquisition and use of automation, communication, and information management technology for the supervision and regulation function across the System.

Figure 2
Supervision and Regulation Information Technology Management Structure



C&CA created an Information Systems Section (ISS) in 1993. ISS's major objectives are to develop information systems policy for the division; direct the development and implementation of analysis capabilities and systems for HMDA and CRA data while ensuring adequate, useful public access to the data; analyze and determine divisionwide information system requirements; direct divisionwide information systems activities, including day-to-day assistance with distributed processing issues; evaluate products and services; enhance and maintain the division's mainframe data systems; and develop and implement Board and Systemwide automation initiatives. For 1997, ISS's operating and capital budget totals about $1.7 million, with five authorized positions and two rotational positions for IRM staff.

In addition to ISS, C&CA relies on IRM to develop and maintain a reliable and stable client/server infrastructure, as well as to manage the C&CA network. Specifically, IRM provides installation, configuration, and maintenance of the client/server network software and hardware; research, testing, evaluation, and integration of new software and hardware releases and components; performance tuning and optimization; enhancement and maintenance of a backup and recovery system; contingency support; support for mainframe and InterFed connectivity; and workstation configuration troubleshooting and problem resolution.[5] These functions are divided among four IRM units, which support C&CA as well as other divisions and offices. The LAN Systems and Support Unit is responsible for network maintenance and support, which includes system administration, performance, and backup and recovery functions. The Distributed Software Support Unit helps install and configure new workstations and provides electronic mail support. The Advanced Technology Unit's security group is responsible for Boardwide security administration. Finally, the Help Desk Call Center in the Central Operations Unit addresses information technology questions or problems.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted audit fieldwork from May to July 1997. Our audit objectives were to determine if C&CA has (1) established an effective process for planning, organizing, directing, and controlling the activities related to distributed processing, (2) adequately managed the efficiency of its local area networks and developed an effective problem management system, (3) properly secured its distributed systems and data, and (4) developed appropriate backup and disaster recovery procedures.

To accomplish our audit objective, we focused on activities performed by C&CA's ISS and the related support provided by IRM. We evaluated network access and security functions provided by Windows NT, and we reviewed Windows NT interfaces with SQL and access controls over three application databases, two of which contain restricted data. Also, we reviewed policies, procedures, and related documentation, interviewed Board staff, and performed various tests. Specifically, we reviewed automation strategic plans, the system configuration diagram, problem tracking logs, various system security reports, and C&CA's contingency plan documents; we also interviewed officers, managers, and staff from C&CA and IRM. To gain a general understanding of user perceptions regarding C&CA distributed processing, we distributed an office automation survey to seventy C&CA LAN users and received forty responses. After analyzing the survey results, we provided a summary of the results to C&CA management. We used security assessment software to test the status of Windows NT security options set for the C&CA server. We also evaluated problem management activities by selecting a sample of the problems logged during 1997 and then contacting the users to discuss their experiences. Finally, we selected a sample of workstations to observe physical security and to discuss logical security, virus protection, installed software, and backup procedures with the users. Our audit was conducted in accordance with generally accepted government auditing standards.

[5] InterFed is a wide area network that provides inter-District LAN connections for the Federal Reserve System.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

In establishing ISS, C&CA has provided its staff with a resource team specifically dedicated to meeting the staff's needs for office automation and application development, as well as a central resource for C&CA information systems policy and direction. C&CA managers and staff who responded to our survey were generally satisfied with the support and assistance provided by ISS. Further, ISS has used innovative approaches to train and support C&CA staff by communicating "Tips of the Week" and a quarterly ISS newsletter over the Board's Intranet and by conducting "Seminars of the Month" to highlight and address current technology topics. ISS has also taken steps to understand and address ISM requirements. It has drafted a matrix that summarizes how it plans to meet ISM requirements and, at the time of our review, had initiated an information security campaign to inform C&CA staff about new information handling procedures. ISS has been actively involved in the System, Board, and interagency information technology efforts; that involvement has helped promote the effective use of information technology to support C&CA's mission.

While ISS has done a commendable job of providing technical support and user education during its first four years of operation, ISS now needs to expand its role in directing the security and administration of its distributed processing environment.   More specifically, we believe ISS needs to define, document, and communicate to IRM the system administration and security expectations that C&CA has for its distributed processing environment. IRM provides the network and file server infrastructure essential for C&CA information processing and communications; a strong partnership between ISS and IRM is needed to maintain a reliable distributed processing environment that is in full compliance with the ISM. In addition, with C&CA's expanding involvement in System and interagency information technology initiatives, we believe that developing an automation strategic plan for the division will better enable C&CA to address future requirements. We further believe streamlining certain aspects of ISS office automation support can free up resources to focus on more strategic issues and application development.

We also found that security controls over C&CA's distributed processing network need improvement and that many of the security features provided by the Windows NT operating system have not been implemented. We believe these security weaknesses stem, in large part, from the transition to a more complex Windows NT environment at both the workstation and file server level; in addition, we noted unclear expectations over the division of responsibility between C&CA and IRM. We also found opportunities to strengthen general controls over C&CA's office automation environment.

The following five recommendations address our observations and findings.

1. We recommend that the Director of C&CA develop a service-level agreement with IRM that defines and documents roles, responsibilities, and expectations for network and security administration.

As the information owner, C&CA is ultimately responsible for managing its information resources and ensuring compliance with policies and safeguards.   To carry out this responsibility, C&CA manages its workstations and depends on IRM to administer the network and file servers that support C&CA's distributed processing and communications. As described on page 5, IRM relies on four separate units to provide this system administration support. With so many different groups involved in various aspects of C&CA's distributed processing, we believe that roles, responsibilities, and expectations need to be clearly defined and communicated and that communication needs to occur on an ongoing basis. However, we found that confusion exists between C&CA and IRM over roles, responsibilities, and expectations for C&CA's distributed processing environment and that communication regarding network and security administration is infrequent.

The following examples illustrate why roles and responsibilities need to be clarified between C&CA and IRM.

— C&CA assumes that IRM handles the technical aspects of ensuring that the Board's client/server infrastructure and wide area network (which supports distributed processing for C&CA and other divisions and offices) complies with the ISM. C&CA officials told us that they contracted with IRM for system and network support and have little or no role themselves in network administration. IRM, however, views ISS as the network administrator for C&CA distributed processing and has certain expectations about the roles that C&CA should play.

— To help eliminate storage-related problems on a file server, C&CA asked IRM to monitor disk space availability. IRM said that it did not have the tools to provide this service, causing C&CA to develop a "homegrown" program that notifies ISS staff when disk space becomes low. An IRM official later told us that IRM staff could have acquired the necessary tools to provide this service if the benefits outweighed the costs, but that they were unaware of the magnitude of the problem.

— According to the ISM, information owners are responsible (a) for ensuring that methods for detecting unauthorized access are in place and (b) for performing periodic reviews on controls. The information custodians are responsible for reporting unauthorized access attempts to information owners, who then review and reconcile security violations. However, at the time of the audit, C&CA had not reviewed controls or requested reports on security violations, and IRM had not provided information or reports to allow C&CA to review and reconcile any violations.

To improve communications and clarify expectations, we believe that C&CA should negotiate a service-level agreement with IRM that describes their respective roles and responsibilities in regard to C&CA distributed processing and security administration, including the services that will be provided and the expected quality of service delivery for areas such as network availability, security, and problem resolution. A service-level agreement typically outlines the service objective, the parties involved, the points of contact, the specific responsibilities, the performance measures, escalation guidelines for handling disagreements or problems, renegotiation guidelines for handling changes to the service-level agreement, and enforcement or compliance considerations for handling deviations from the agreement. We believe that negotiating a service-level agreement with IRM would help each party clarify and manage roles, responsibilities, and expectations; provide a basis for monitoring support provided; help ensure accountability; and foster increased communication and partnership.

2. We recommend that the Director of C&CA develop a formal office automation strategic plan for the division's distributed processing environment.

C&CA does not have an "office automation" strategic plan that collectively addresses information technology requirements and the broader distributed processing infrastructure issues that have a direct impact on C&CA applications. According to ISS, distributed processing strategic planning is basically a subset of the planning performed by each of the business functions. While we agree that business processes should drive automation, we believe that C&CA also needs a strategic view of its distributed processing program to ensure that it will be able to support these individual data processing requirements when taken as a whole and to address future division and System initiatives in a timely manner.

A formal office automation strategic plan would also foster increased coordination with other offices and divisions. During the audit, we found that little coordination occurs between C&CA and IRM regarding Boardwide infrastructure issues that have or will have a direct and long-term impact on C&CA's distributed processing environment. For example, C&CA was not aware at the beginning of our audit that IRM had fully implemented NT as the file server platform supporting C&CA distributed processing and did not understand how NT at the server level would impact their office automation from a more strategic perspective.

C&CA is actively involved in the Board's Distributed Processing Advisory Group, the ITC, and other Systemwide distributed processing initiatives that have a substantial impact on

ISS staff.[6] An automation strategic plan will help ensure that C&CA has the necessary people, hardware, software, and other information resources to meet evolving business needs across the System in a timely and responsive manner, within the overall framework established by the Board. A strategic plan can also help ISS explore and communicate how the new technology and tools can be leveraged to better work with C&CA management and users in achieving their business objectives.

3. We recommend that the Director of C&CA streamline and increase the efficiency of ISS's technical support by (a) restructuring the process for providing user technical assistance, and (b) developing and implementing an improved software distribution process.

Providing users with technical assistance is a high priority in C&CA and a multi-layered, user support structure has evolved to meet this need. Each member of ISS is responsible for providing technical assistance to users and for individually recording these "service calls" in narrative form as part of his/her monthly status report. In addition, the IRM Help Desk is responsible for addressing questions from the ISS, as well as from individual C&CA users. The Help Desk maintains tracking sheets for hardware problems and a separate log for software problems—each on a Boardwide basis. IRM's LAN Systems and Support Unit is also responsible for handling network-related questions, and it maintains a separate internal log on a Boardwide basis.

While it appears to be responsive to user needs, ISS recognizes that the current process is inefficient and has hidden costs. ISS staff told us they were frequently interrupted to handle user questions, making it difficult to focus on applications development and other functions. Because C&CA does not have a comprehensive system or process to measure how many resources it is devoting to problem resolution, it is difficult for management to identify the costs associated with providing user support or to analyze trends.

We believe that C&CA needs to restructure its technical assistance process to make it more efficient and effective. First, C&CA needs more meaningful information on the scope and type of technical support currently being provided by ISS and IRM, including the resources that are being devoted to problem resolution. Creating a problem database that includes information such as the date the problem was opened, a description of the problem, the diagnosis, the analyst assigned the problem, its priority, the status of the problem, the anticipated resolution date, the action taken, and the actual resolution date will allow C&CA to analyze a wide range of issues. For example, the database can be used to generate reports that classify problems into categories (such as hardware, network, new user,

[6] The Distributed Processing Advisory Group, which is composed of representatives from various Board offices and divisions, is responsible for defining and coordinating the implementation of the Board's automation and telecommunications architecture.

relocation, and software problems) and that give insights into the complexity of the issues and the time spent in resolving them. More formal coordination between ISS, the IRM Help Desk, and the LAN Systems and Support Unit will also provide a more complete picture of the scope of technical support being provided to C&CA staff.

Once C&CA has this information, the next step is to review the scope of services being provided and determine if this scope is consistent with division goals and objectives. For example, C&CA may find that some of the services it is providing through its technical support function could be more efficiently and effectively handled by more focused training, clearer procedures, or increased coordination with IRM. The information will also help C&CA in defining the service level and coverage that it would like to provide through its technical support function and the types of training that the technical support staff will need to meet these requirements.

In addition to the time they invest in providing technical support, ISS staff told us that software upgrades consume a substantial amount of their time, which is typical of many organizations. According to the Gartner Group, updating software products generally accounts for 55 percent of a desktop system's total cost during a five-year period.[7] Gartner Group also notes that the task is manual and tedious, and many organizations respond by limiting the update frequency or shifting the problem to end users.[8]

We believe that ISS should review various alternatives for upgrading division software with the goal of freeing up ISS resources to work on more substantive issues. For example, electronic software distribution tools may offer a cost effective solution. According to the Gartner Group, a good electronic software distribution package not only distributes and installs software, but also provides capacity checking and auditing and management reports. An alternative may be to include the software upgrade distribution process in the service-level agreement negotiations with IRM.

4. We recommend that the Director of C&CA improve security controls over C&CA's distributed processing environment by defining C&CA's data security requirements and working with IRM to ensure compliance with the *Information Security Manual*.

The ISM defines the Federal Reserve System's security policies and safeguards in order to protect information assets from unauthorized access, modification, destruction, or

[7] Gartner Group Inc. is an independent advisor of research and analysis regarding information technology industry developments and trends.

[8] D. Cappuccio, W. Kirwin, and L. Pawlick, *Total Cost of Ownership: Reducing PC/LAN Costs in the Enterprise*, Strategic Analysis Report, Network Computing Infrastructures, February 9, 1996, Gartner Group Inc., 1996.

disclosure. Under the ISM, all Federal Reserve System officers, employees, consultants, and contract personnel are responsible for adhering to and supporting ISM policies and safeguards. Specific roles and responsibilities are assigned based upon the information security organizational structure and the information ownership. As the information owner, C&CA's responsibilities include making decisions concerning the classification, use, and protection of information; authorizing access to information; ensuring that methods for detecting unauthorized attempts are in place; reviewing and reconciling security violations; and performing periodic reviews of controls to ensure that information is only available to persons with a need to know. As the information custodian, IRM's responsibilities include consulting with the information owners to ensure that appropriate security controls are implemented, administering logical access to information as approved by the information owner, and reporting unauthorized access attempts to owners.

Properly securing the Windows NT operating system in a manner consistent with the ISM requires extensive customization because most of the NT security features are turned off when the system is installed. Based on our review of IRM's implementation of the Windows NT operating system to manage and secure C&CA applications and data, we found that security controls over the distributed processing network supporting C&CA need improvement and that many of the security features of the Windows NT operating system have not been implemented. Security controls need to be strengthened in the following three areas:

1) Providing more consistent implementation of NT access controls (i.e, passwords),

2) Separating the duties of the SQL system and security administrators, and

3) Restricting access to application databases and operating system software and tables.

The detailed technical findings and recommendations for corrective action in each of these areas have been reported in a separate letter to the Director of C&CA and the Director of IRM.

We believe many of these security weaknesses occurred because C&CA recognized only its responsibility for authorizing access to information and assumed that IRM, as information custodian, would properly define access controls for C&CA's information system. C&CA officials told us that they believed that IRM would appropriately secure the distributed environment in a manner comparable to the security levels implemented for the Board's mainframe environment, and so did not explicitly state security requirements.

To meet its ISM responsibilities and to adequately manage and secure its information, we believe that C&CA needs to perform a security application "walk through" with IRM's Data Security group and its LAN Systems and Support Unit. Such a walk through would allow C&CA to develop a working knowledge of the security capabilities of the operating system and the database management system, which are the key security components of C&CA's

distributed processing system. By obtaining a basic understanding of the underlying security features, C&CA will be better able to develop more comprehensive procedures for authorizing access to its information, perform periodic reviews of controls to ensure that information is available to persons with a "need to know," and review and reconcile security violations.

5. We recommend that the Director of C&CA improve general controls over the distributed processing environment by (a) terminating procedures that require users to share their passwords with ISS and updating the division's *Information Security Procedures* to reflect the ISM requirements, (b) documenting application development standards, (c) formalizing procedures for maintaining information on software licenses, and (d) reviewing and testing IRM's backup procedures on a regular basis and completing the division's disaster recovery plan.

General controls apply to all computer processing environments and are necessary to ensure that applications run in a controlled and secure environment. During the course of our audit, we found opportunities to improve C&CA's general control framework for distributed processing in a number of areas, as described below. Clear and well-documented policies and procedures in each of these areas can help ensure that the C&CA distributed processing environment is secure from unauthorized access.

Access and Data Security Controls

Under its current access control procedure, ISS semiannually sends a memo to users in the division requiring them to change their workstation password, record the new password on a "password recording form," and return this form to ISS staff under a RESTRICTED FR cover sheet. An ISS staff member then logs the user passwords into a password-protected database on his/her workstation. A hard copy of the user passwords is then distributed to ISS staff, under a RESTRICTED FR cover, in case they need to access files on a user's workstation when that user is not in his/her office. ISS officials believe that this procedure is necessary because it allows them to verify that users change their passwords at least semiannually and it facilitates ISS support of the workstations even when users are out of the office.

Maintaining a database and hard copy listing of all C&CA user passwords greatly compromises security and places the division in noncompliance with the ISM, which requires that the privacy and integrity of passwords be maintained and prohibits sharing of passwords. Anyone who gains access to either the hard copy or the electronic version of the password listing would virtually assume full and open access to every user account in the division. Effectively managing password security is particularly important in a distributed processing environment, and we believe that C&CA should terminate its current procedures immediately.

At the time of our review, C&CA was implementing its information security campaign to orient staff to the new procedures for handling Board classified material and had also planned to update its internal policies and procedures. However, we found that the policies and procedures had not yet been updated to reflect the information classification categories defined in the ISM, or to include information or guidance on virus scan protection, copyright policy, and personal software usage.

Software Development and Maintenance Controls

Although ISS is responsible for developing software systems and applications, it does not have documented application development standards. Application development standards are an important general control for ensuring the integrity of business application systems over the system life cycle. Lack of application development standards may result in weak security, incompatible or inefficient systems, redundant systems, or reliance on inaccurate information. In addition, formalizing and documenting application development standards would help ISS provide consistent guidance to each ISS staff member, at each level of skill and experience.

Software Licensing Controls

Effectively managing information on software licenses is another important general control. Misuse of software can result in penalties, and improperly tracking software can lead organizations to inadvertently pay duplicate licensing fees. When we discussed C&CA procedures for ensuring compliance with the software license agreements, we found confusion in how software license information is maintained and how ISS ensures compliance with software licenses. Although ISS recognizes the need to track software licenses and had developed a software inventory database to assist in the process, it does not yet have a formal system that clearly links the software inventory with the applicable licenses. A more comprehensive system would help ISS verify that C&CA is purchasing the correct number of software licenses and is in full compliance with licensing agreements for the software it has purchased.

Backup Procedures and Disaster Recovery

C&CA relies on IRM to maintain its network environment and provide day-to-day file backup and recovery services. Although IRM has documented off-site backup procedures for C&CA's distributed processing, some users raised questions about whether these backup and recovery processes work as intended. Because backup procedures are important for contingency planning as well as day-to-day operations, we believe C&CA should review and test IRM's backup procedures on a regular basis to ensure they meet the division's needs.

IRM also serves as the focal point for developing an "umbrella," Boardwide information systems contingency and business resumption plan, of which C&CA is a part. In the event of an emergency or disaster, contingency and business resumption plans provide the critical framework for recovering systems and operations in an orderly and timely manner. C&CA is in the process of modifying the IRM contingency planning model to better meet its needs. For example, C&CA wants to develop a checklist that describes the steps to take in a contingency situation and lists who is responsible for taking them. Although the initial documentation for the checklist appears thorough, at the time of our review, ISS had not begun gathering the specific information that it will need to compile the checklist. Because an emergency situation can happen at any time, we believe C&CA should take steps to expedite and complete the division's disaster recovery plan.

ANALYSIS OF COMMENTS

The Director of C&CA's response to our draft report indicates general agreement with the five recommendations (see appendix 1). The response also reflects C&CA's position that some of the points raised in our report are the result of systemic issues that could be more efficiently addressed on a Boardwide basis. C&CA's response indicates that it expects IRM to be proactive in providing at least a basic level of service. For example, while C&CA agreed with our recommendation to develop a service-level agreement with IRM, they observed that a blanket service-level agreement covering common services (such as physical security of file servers) provided by IRM to its clients would be more efficient than a C&CA only service-level agreement. They added that services unique to a division would be included in division-specific, service-level agreements.

We continue to emphasize that, as the information owner, C&CA is ultimately responsible for managing its information resources and ensuring compliance with polices and safeguards. As a result, C&CA must take responsibility for defining what level of performance it expects from IRM and work with IRM to ensure C&CA requirements are met.

APPENDIXES

Appendix 1 - Division's Comments

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

RESTRICTED FR

MEMO

DATE: December 12, 1997

TO: Barry R. Snyder

FROM: Griffith L. Garwood

SUBJECT: Response to Inspector General's Draft Report on the Audit of the Division of Consumer and Community Affairs' Distributed Processing Environment (A9704)

We reviewed the draft Report on the Audit of the Division of Consumer and Community Affairs' Distributed Processing Environment (A9704) dated November 24, 1997 and completed an analysis of the recommendations. Overall, we agree with your findings. Below is the Division of Consumer and Community Affairs' (C&CA) responses to the five recommendations found in the draft report; the recommendations are in bold face, followed by our responses.

Recommendation 1: We recommend that the Director of C&CA develop a service-level agreement with IRM that defines and documents roles, responsibilities, and expectations for network and security administration.

We agree, but believe that a service-level agreement alone will not ensure compliance with policies and safeguards. (The present "enterprise services agreement" between IRM and client divisions already functions as a service-level agreement.) Since the present service-level agreement appears to have been inadequate, we recommend that a periodic audit also be conducted that focuses on how IRM manages networks for client divisions (i.e., whether IRM is in compliance with the requirements of the Information Security, the Distributed Processing Security Support, and the Mainframe and FEDNET Security Support Manuals.)

We also believe that a blanket service-level agreement covering common services provided to clients by IRM rather than a C&CA only service-level agreement is a more efficient avenue. Physical security of file servers is an example of a common service that would be included in a blanket agreement. Services that are unique to a division would be included in division-specific service-level agreements.

Appendix 1 - Division's Comments

RESTRICTED FR

We agree that C&CA should review security violation reports and security controls regularly, but we believe that IRM should notify the user division immediately when a violation occurs. In addition, we believe that IRM should design violation reports that could be used by all divisions it supports, and that it would be more efficient for IRM to distribute the reports regularly rather than have divisions request reports at different intervals.

Recommendation 2: We recommend that the Director of C&CA develop a formal office automation strategic plan for the division's distributed processing environment.

We agree.

Recommendation 3: We recommend that the Director of C&CA streamline and increase the efficiency of ISS's technical support by (a) restructuring the process for providing user technical assistance, and (b) developing and implementing an improved software distribution process.

We agree. C&CA plans to contract technical assistance services with an outside vendor and will implement new procedures for logging service calls. Also, C&CA has been informed that IRM will begin testing distribution software in 1998; C&CA asked to be included in the pilot.

Recommendation 4: We recommend that the Director of C&CA improve security controls over C&CA's distributed processing environment by defining C&CA's data security requirements and working with IRM to ensure compliance with the Information Security Manual.

We agree, but we believe that issues involving security controls and the distributed processing area are not limited to C&CA. Moreover, C&CA believes that it is not unreasonable to expect IRM to implement security controls appropriately, especially since the enterprise services agreement between IRM and client divisions indicates that security is one of the services provided by IRM.

Recommendation 5: We recommend that the Director of C&CA improve general controls over the distributed processing environment by (a) terminating procedures that require users to share their passwords with ISS and updating the division's Information Security Procedures to reflect the ISM requirements, (b) documenting application development standards, (c) formalizing procedures for maintaining information on software licenses, and (d) reviewing and testing IRM's backup procedures on a regular basis and completing the division's disaster recovery plan.

We agree with the recommendation to terminate the procedures that require users to share their passwords with the division's Information Systems Section. C&CA has taken steps

Appendix 1 - Division's Comments

RESTRICTED FR

to implement this recommendation--network passwords are no longer collected. However, C&CA will continue collecting Ontime, cc:Mail, and power-on passwords until new password handling procedures are implemented by C&CA in February 1998.

We agree with the recommendation to update C&CA's Information Security Procedures to reflect ISM requirements. C&CA will continue to follow its ISM compliance matrix and should be in compliance by the end of June 1998.

Although we agree with the recommendation to document application development standards, C&CA believes these standards should be uniform across Board divisions. (The Distributed Processing Advisory Group could recommend standards to the Automation Policy and Programs Committee, which could act on and issue standards.) In the interim, however, C&CA will develop basic application development standards that will include standards for requirements gathering, testing, documentation, and security.

We agree with the recommendation to formalize maintaining software licensing. Software licensing controls are being included as part of the distribution software project. As stated earlier, IRM is leading this project with C&CA as a test division.

We agree with the recommendations about backup and recovery procedures; C&CA will take steps to implement backup and disaster recovery procedures by the end of February 1998.

cc: B. Bowen
P. Kelley
B. Coleman
M. English
T. Price

Appendix 2 - Principal OIG Contributors to this Report

- Bonnie Smolak, Senior EDP Auditor and Auditor-in-Charge
- Beth Coleman, Senior Auditor
- Gary Lester, Senior EDP Auditor
- Diana Falcigno, Associate EDP Auditor
- Pam Debnam, Senior Secretary
- Patty Kelley, Audit Manager